The Bell System Technical Journal
Vol. 55, No. 4, April 1975
Printed in U.S.A.

Toward a Group-Theoretic Proof of the Rearrangeability Theorem for Clos' Network

By V. E. BENEŠ

(Manuscript received October 8, 1974)

Methods from group theory and combinatorics are used to prove the (Slepian-Duguid) rearrangeability theorem for Clos' three-stage network. The nr-permutations realizable in such a network can be represented as a product $G\varphi^{-1}H\varphi G$, where G, H are subgroups realized by stages and φ is the special cross-connect field used in making frames. Thus, rearrangeability can be cast as $G\varphi^{-1}H\varphi G = S_{nr}$ = symmetric group of degree nr. Since it is an elementary theorem that a permutation group containing all transpositions is symmetric, it is enough to show that the product $G\varphi^{-1}H\varphi G$ is closed under multiplication and contains all transpositions. We prove that closure of the product is equivalent to a property of suitable partitions: existence of systems of common representatives. This property, formulated by J. B. Kruskal, is a consequence of Hall's theorem on distinct representatives. It is easily seen that $G\varphi^{-1}H\varphi G$ contains all transpositions, so the Slepian-Duguid theorem follows.

I. INTRODUCTION

In this paper we continue the exploration hegun in previous work[1–3] of the relationships hetween permutation groups and connecting networks that are made of stages, frames, and cross-connect fields. Our results concern a well-known theoretical result of this area, the Slepian-Duguid theorem, which states that Clos' three-stage network with square switches is rearrangeable, i.e., realizes any permutation. Since the permutations realizahle hy a stage form a special kind of subgroup, the theorem has heen viewed in terms of group theory as a factorization of the symmetric group S_{nr} of degree nr into a product of three suhgroups or, alternatively, into a product of two mutually inverse double cosets.[3]

We further illuminate this basic rearrangeability theorem hy giving it as nearly group-theoretic a proof as we have been able to find. This proof starts from the known characterization[1] of the nr-permutations

realizable by a Clos' three-stage network as a product $G\varphi^{-1}H\varphi G$, where G, H are subgroups realized by stages and φ is a "canonical" cross-connect field. It then shows that this product is closed under multiplication, and that it contains all nr-transpositions, whence immediately, by an elementary theorem, that it contains any nr-permutation, i.e., that $S_{nr} = G\varphi^{-1}H\varphi G$.

In the course of this proof we show that the basic combinatorial backbone of the rearrangeability theorem is really the existence of systems of common representatives (SCRs) for pairs of partitions. Since, in apparent contrast, Duguid's original proof[4] used Hall's theorem on systems of distinct representatives (SDRs) of subsets, we have also sought to clarify just how the rearrangeability result depends on Hall's theorem. The contrast above is apparent only because there are standard ways of proving SCR results from SDR results. In the present context, the two approaches are equivalent and lead to the same results. However, the SCR formulation is closer to the group-theoretic aspects than is Duguid's original SDR proof: it provides an SCR property that is a consequence of Hall's theorem and is necessary and sufficient for the product $G\varphi^{-1}H\varphi G$ to be closed. The property was first formulated by J. B. Kruskal in unpublished notes about rearrangeable networks dating from 1964.

II. SETTING AND FORMULATION

We now sketch the group-theoretic interpretation of the Slepian-Duguid theorem in some detail, as has been done in earlier work.[3] Figure 1 shows Clos' three-stage network, composed of three sym-

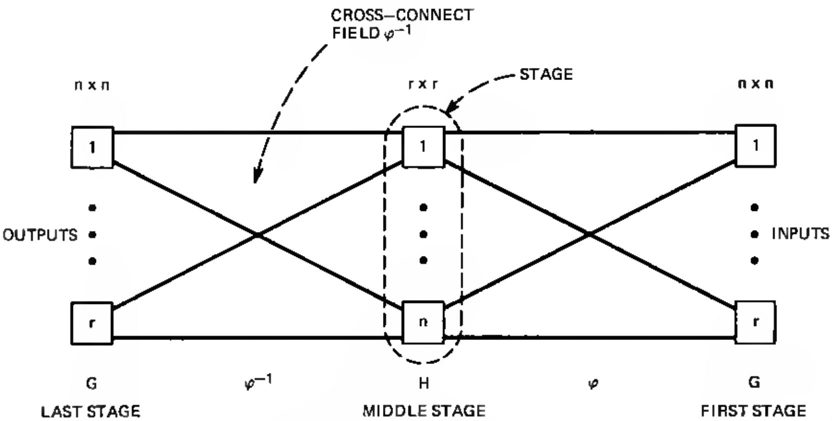

Fig. 1—$G\varphi^{-1}H\varphi G$ describes the permutations realizable by Clos' three-stage network.

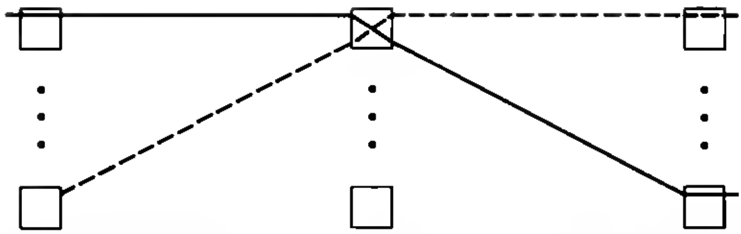

Fig. 2—Getting transpositions in $G\varphi^{-1}H\varphi G$: terminals on different outer switches.

metrically placed stages interconnected by the "canonical" cross-connect field φ and its inverse. Each stage can realize precisely those permutations from a certain subgroup of S_{nr}, depending on the size and number of switches in the stage. The r $n \times n$ switches of each outer stage realize a subgroup G isomorphic to $(S_n)^r$, viz., all those that permute the sets $\{kn + 1, kn + 2, \cdots, (k + 1)n\}$, $k = 0, \cdots, r - 1$, within themselves. A similar statement holds for the center stage, but with n and r interchanged, to define a subgroup H isomorphic to $(S_r)^n$.

Thus, if we think of the network in Fig. 1 as acting from right to left, and if we interpret composition of permutations as left-multiplication of the inner permutation by the outer, then the permutations realizable by Clos' three-stage network with square switches are precisely those in the complex

$$G\varphi^{-1}H\varphi G.$$

The Slepian-Duguid theorem says that this complex is exactly the symmetric group S_{nr} of degree nr. We note for future reference that all transpositions are realizable; this can be seen from Figs. 2 and 3, in which the remaining terminals (not shown) are connected through to "themselves," as is possible and indeed necessary to realize a transposition.

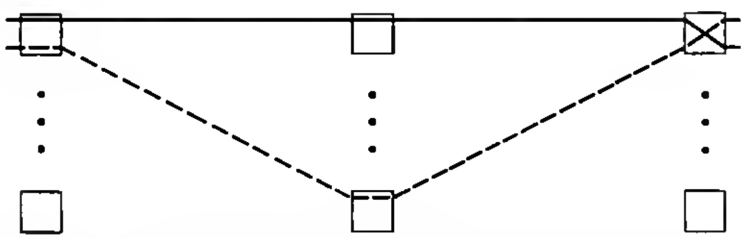

Fig. 3—Getting transpositions in $G\varphi^{-1}H\varphi G$: terminals on same outer switch.

III. SYSTEMS OF DISTINCT REPRESENTATIVES

Let X he a set, and $X_1, \cdots, X_m$ finite suhsets of X. We make the following definition.

Definition 1: Elements $x_1, \cdots, x_m$ from X form a system of distinct representatives (SDR) *of $X_1, \cdots, X_m$ iff $x_i \in X_i$ and $x_i \neq x_j$ if $i \neq j$, for $i, j = 1, \cdots, m$.*

Hall's theorem[5] gives a necessary and sufficient condition for the X_i to have an SDR, thus:

Theorem 1 (Hall): $X_1, \cdots, X_m$ have an SDR *iff for $k = 1, \cdots, m$, the union of any k X_i has at least k elements.*

This result was used by Duguid in his proof of the rearrangeability of Clos' network witb square switcbes. It enabled him to decompose any permutation into a union of submaps each of which, in switching terminology, carried exactly one terminal on each input switch onto images that were spread over all the output switches. These suhmaps could tben he accommodated, one each on a middle switch.

IV. SYSTEMS OF COMMON REPRESENTATIVES

Let $P = \{P_i\}$ and $Q = \{Q_i\}$ he partitions of a set X with $|P| = |Q|$.

Definition 2: A subset $E \subset X$ is called a system of common representatives (SCR) *for P and Q iff*

$$\begin{aligned} |E \cap P_i| &= 1, \qquad P_i \in P \\ |E \cap Q_j| &= 1, \qquad Q_j \in Q. \end{aligned}$$

Ryser[6] gives an SDR argument to prove a necessary and sufficient condition for two partitions as above to have an SCR. In the cases of interest to us here, a sufficient condition can be given in a particularly simple way. We make

Definition 3: Q is an (r, n)-partition iff $|Q| = r$, and $|Q_i| = n$ for $Q_i \in Q$. An (r, n)-partition of X is one into r sets each having n elements.

We use suhstantially Ryser's argument[6] to prove the following special case (Theorem 2.2, p. 51, of Ref. 5) of his result:

Theorem 2: Let P, Q be (r, n)-partitions of X. Then P and Q have an SCR.

Proof: For $j = 1, \cdots, r$, let $A_j = \{i : P_i \text{ meets } Q_j\}$. Take any union of k of tbese sets, $A_{j_1} \cup \cdots \cup A_{j_k}$, and observe that $Q_{j_1} \cup \cdots \cup Q_{j_k}$ has precisely nk elements in it. Hence, at most $r - k$ integers in tbe range $1, \cdots, r$ fail to be in some $A_{j_1}, \cdots, A_{j_k}$. Thus,

$$|A_{j_1} \cup \cdots \cup A_{j_k}| \geqq k, \ .$$

so, hy Hall's theorem, $\{A_j\}$ has an SDR $\{i_j\}$, and $P_{i_j} \cap Q_j \neq \phi$. Hence, P and Q have an SCR.

V. ORTHOGONAL PARTITIONS

We now prove a property of partitions that will later turn out to he equivalent to the closure of the permutations realizahle hy Clos' network.

Definition 3: Partitions P, Q are orthogonal, written $P \perp Q$, iff $P_i \in P$ and $Q_j \in Q$ imply $|P_i \cap Q_j| = 1$.

Remark: If $P \perp Q$, and π is a permutation, then $\pi P \perp \pi Q$.

The next result was first given hy J. B. Kruskal.

Theorem 3: If P, R are both (r, n)-partitions, then there is an (n, r)-partition Q orthogonal to each of P and R.

Proof: By Theorem 2, P and R have an SCR Q_1. Remove all elements of Q_1 from the P_i and the Q_j to give new $(r, n - 1)$-partitions P' and Q'. Repeat to find $Q_2, Q_3, \cdots, Q_n$, and then take $Q = \{Q_i\}$.

It is convenient to have notations for three special partitions which arise naturally from the switching applications we are making. Clearly, the inlets (or outlets) of the network in Fig. 1 can be partitioned according to what last (or first) stage switch they are on. Similarly, the "wires" of the cross-connect fields between the stages can be partitioned according to what middle switch they impinge on. Accordingly, we define the (r, n)-partition S (hy "outer" switches) as

$$S = \{S_j, j = 1, \cdots, r\}, \qquad S_j = \{k: (j - 1)n < k \leqq jn\},$$

and the (n, r)-partition M (hy "middle" switches) as

$$M = \{M_j, j = 1, \cdots, n\}, \qquad M_j = \{k: (j - 1)r < k \leqq jr\}.$$

It is also convenient to partition by terminal position on outer switches, so we define the (n, r)-partition T by $T = \{T_j, j = 1, \cdots, n\}$ with

$$T_j = \{k: k = ln + j \quad \text{for some} \quad 0 \leqq l \leqq r - 1\}.$$

The canonical cross-connect field is defined hy

$$\varphi: j \to 1 + \left[\frac{j - 1}{n}\right] + r[(j - 1) \bmod n] \qquad j = 1, 2, \cdots, nr.$$

The following properties can he verified: $\varphi T = M$, $S \perp T$. Intuitively, φ takes the jth terminal on the ith switch into the ith terminal in the jth switch.

VI. CHARACTERIZATION OF REALIZABLE PERMUTATIONS

The next theorem will give a necessary and sufficient condition on a permutation π to be realizable in Clos' network, i.e., to belong to $G\varphi^{-1}H\varphi G$. We start with a lemma.

Lemma: Let P be any (r, n)-partition. If there is an (n, r)-partition R such that

$$P \perp R \perp S,$$

then there exists an element $g \in G$ such that

$$\varphi g P \perp M.$$

The practical import of this result is as follows: Consider a frame of r $n \times n$ switches followed by n $r \times r$ switches, with the canonical cross-connect field φ in between (Fig. 4); then, under the hypothesis there is a setting of the right-hand switches (i.e., the r $n \times n$), which has the effect of connecting each set of P to some terminal on every switch of the left-hand stage of n $r \times r$, i.e., it images each P_i so as to reach every left switch (exactly once).

Proof of lemma: Let $R = \{R_i\}$. Each R_i is simultaneously an SNR of P and one for S. Thus, if we connect the terminals of R_1 to the first left-hand stage switch, we will have used up one terminal from each P-set and also one from each switch on the right. This procedure can be repeated with $R_2, R_3, \cdots, R_n$ to give the result. Evidently, this set of connections defines an element $g \in G$ such that each set of $\varphi g P$ is spread over the left-hand stage switches, i.e., such that $\varphi g P \perp M$.

Theorem 4: $\pi \in G\varphi^{-1}H\varphi G$ *iff there is an (n, r)-partition R such that*

$$S \perp R \perp \pi^{-1}S.$$

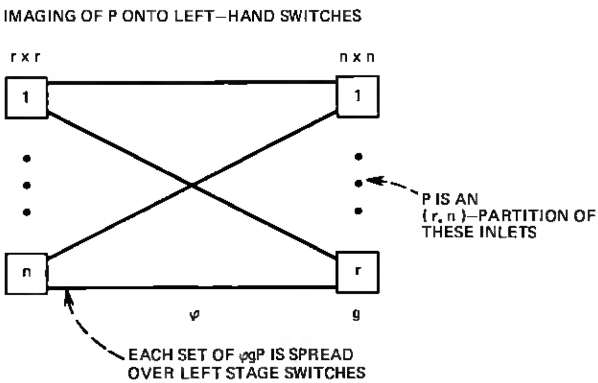

Fig. 4—Import of the lemma.

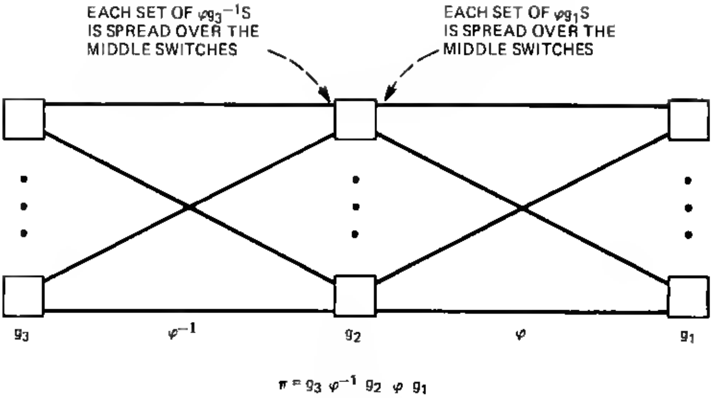

Fig. 5—$\varphi g_1 S \perp M \perp \varphi g_3^{-1} S$.

Proof: Let M be the partition of nr by middle switches, i.e., the (n, r)-partition consisting of the n sets

$$\{jr + 1, jr + 2, \cdots, (j + 1)r\} \qquad J = 0, 1, \cdots, n - 1,$$

and note that $hM = M$ for $h \in H$. Suppose now that $\pi \in G\varphi^{-1}H\varphi G$ with $\pi = g_3\varphi^{-1}g_2\varphi g_1$ and g_1, $g_3 \in G$, and $g_2 \in H$. It can be seen from Fig. 5 that each set of $\varphi g_3^{-1}S$ is spread over all the middle switches. Similarly, each set of $\varphi g_1 S$ is spread over the middle switches. Combinatorially, and without the help of pictures, these facts follow from $\varphi T = M$, from $gS = S$ for $g \in G$, and from $S \perp T$, and they can be rendered as

$$\varphi g_1 S \perp M$$
$$\varphi g_3^{-1} S \perp M.$$

It follows from the observation above that $g_2 M = M$, and thus, by the remark after Definition 3,

$$g_2\varphi g_1 S \perp M \perp \varphi g_3^{-1} S,$$

whence

$$\pi S \perp g_3\varphi^{-1} M \perp S$$

or

$$S \perp g_1^{-1}\varphi^{-1}g_2^{-1}M \perp \pi^{-1}S.$$

For R, we take $g_1^{-1}\varphi^{-1}g_2^{-1}M$, and the necessity is proved.

For the sufficiency, we use the lemma, according to which the hypothesis implies that there is an element $g_1 \in G$ such that

$$\varphi g_1 \pi^{-1} S \perp M.$$

Thus, in Fig. 5, by setting up g_1 in the right-hand stage, we can connect,

for each $j = 1, \cdots, n$, the terminals of $\pi^{-1}S_j$, one each to a middle switch. It remains to define g_2 for the middle stage by collecting those destined for $S_1, S_2, \cdots$, and g_3 for the left-hand stage by distributing within each of the sets $S_1, S_2, \cdots$ in the left-hand stage. This is done precisely as follows: Define g_2 by switching a terminal l to third stage switch j iff

$$l \in \varphi g_1 \pi^{-1} S_j.$$

It follows that $\varphi^{-1} g_2 \varphi g_1 \pi^{-1} S_j = S_j$. Then define g_3 by switching, within each final switch, $\varphi^{-1} g_2 \varphi g_1 \pi^{-1} i$ to i. Then $\pi = g_3 \varphi^{-1} g_2 \varphi g_1 \in G \varphi^{-1} H \varphi G$, as was to be proved.

VII. CLOSURE AND FACTORIZATION

Theorem 5: *$G\varphi^{-1}H\varphi G$ is closed under multiplication iff, for any two (r, n)-partitions P, Q, there is an (n, r)-partition R such that $P \perp R \perp Q$.*

Proof: Let P, Q be given (r, n)-partitions. If $G\varphi^{-1}H\varphi G$ is closed, then it is a group that contains all transpositions, and so equals S_{nr}. Hence, there exist permutations π_1 and π_2 such that

$$\pi_1 S = P, \qquad \pi_2^{-1} S = Q.$$

Since $G\varphi^{-1}H\varphi G$ is closed, it is clear that $\pi_2\pi_1$ belongs to it. By Theorem 3, or by inspection of Fig. 5, with $\pi = \pi_2\pi_1$, we see there is a partition N such that

$$S \perp N \perp (\pi_2\pi_1)^{-1} S;$$

that is,

$$\pi_1 S \perp \pi_1 N \perp \pi_2^{-1} S.$$

For the requisite partition R, take $\pi_1 N$, and the necessity is proved.

For the sufficiency, let $\pi_1, \pi_2 \in G\varphi^{-1}H\varphi G$, and let $P = \pi_1 S$, $Q = \pi_2^{-1} S$. Then, by the hypothesis, there is an (n, r)-partition R such that

$$P \perp R \perp Q;$$

that is,

$$\begin{aligned} \pi_1 S \perp R \perp \pi_2^{-1} S \\ S \perp \pi_1^{-1} R \perp (\pi_2\pi_1)^{-1} S. \end{aligned}$$

Hence, by Theorem 4, $\pi_2\pi_1 \in G\varphi^{-1}H\varphi G$, and we have proved that $G\varphi^{-1}H\varphi G$ is closed.

Theorem 6 (Slepian-Duguid):

$$S_{nr} = G\varphi^{-1}H\varphi G.$$

Proof: Immediate from Theorems 3 and 5, since the right-hand side contains all transpositions and is closed.

VIII. FURTHER PROBLEMS AND COMMENTS

Since H is a group, it follows that $\varphi^{-1}H\varphi$ is also a group, one conjugate to H, and that the Slepian-Duguid theorem can be cast as a decomposition

$$S_{nr} = \bigcup_{\pi \in \varphi^{-1}H\varphi} G\pi G$$

into disjoint double cosets, similar to the classical Frobenius[7] decomposition. It is tempting to expect some sort of connection with Frobenius' theorem here. One can speculate, in particular, that there is a proof of the Slepian-Duguid theorem from Frobenius', obtained by specializing the requisite cosets to those of the form $G\pi G$ with π in the conjugate $\varphi^{-1}H\varphi$, and showing that only these need be considered.

In conversation, Richard Stanley has indicated that, in another problem, also concerned with showing that a certain set of generated permutations was all of S_{nr}, he had used the known result that a primitive group containing a transposition is a symmetric group. His remark stimulated our original approach to a "group-theoretic" proof of the rearrangeability theorem: one easily shows that, if $G\varphi^{-1}H\varphi G$ is a group, then it is a primitive group containing a transposition; the problem then became to show that it was closed, a property that turned out to be equivalent to Kruskal's orthogonal partitions result (Theorem 3). Since closure was by comparison difficult to prove, and since it became clear that $G\varphi^{-1}H\varphi G$ contains all transpositions, the simpler proof presented here could be used, making the original side trip via primitive groups gratuitous. Stanley's idea, however, is still a possible proof method for other networks that lead to less transparent groups of realizable permutations.

REFERENCES

1. V. E. Beneš, "Permutation Groups, Complexes, and Rearrangeable Connecting Networks," B.S.T.J., *43*, No. 4, Part 2 (July 1964), pp. 1619–1640.
2. V. E. Beneš, "Proving the Rearrangeability of Connecting Networks by Group Calculations," B.S.T.J., *54*, No. 2 (February 1975), pp. 423–434.
3. V. E. Beneš, "Applications of Group Theory to Connecting Networks," B.S.T.J., *54*, No. 2 (February 1975), pp. 409–422.
4. V. E. Beneš, *Mathematical Theory of Connecting Networks and Telephone Traffic*, New York: Academic Press, 1965, pp. 86 ff.
5. H. J. Ryser, *Combinatorial Mathematics*, Carus Monograph 14, Math. Assoc. of America, New York: John Wiley, 1963, p. 48.
6. Ref. 5, p. 50.
7. W. Ledermann, *Introduction to the Theory of Finite Groups*, Edinburgh and London: Oliver and Boyd, 1957, p. 60.